

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日      2 0 0 3 年    5 月 2 3 日  
Date of Application:

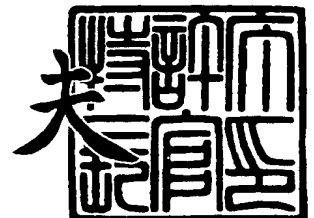
出 願 番 号      特 願 2 0 0 3 - 1 4 6 4 9 1  
Application Number:  
[ST. 10/C]:      [ J P 2 0 0 3 - 1 4 6 4 9 1 ]

出 願 人      株式会社東芝  
Applicant(s):

2 0 0 4 年    2 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 A000301122

【提出日】 平成15年 5月23日

【あて先】 特許庁長官 殿

【国際特許分類】 H01L 21/00

【発明の名称】 データ処理装置及び論理演算装置

【請求項の数】 16

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研  
                            究開発センター内

    【氏名】 藤崎 浩一

【特許出願人】

    【識別番号】 000003078

    【氏名又は名称】 株式会社 東芝

【代理人】

    【識別番号】 100058479

    【弁理士】

    【氏名又は名称】 鈴江 武彦

    【電話番号】 03-3502-3181

【選任した代理人】

    【識別番号】 100091351

    【弁理士】

    【氏名又は名称】 河野 哲

【選任した代理人】

    【識別番号】 100088683

    【弁理士】

    【氏名又は名称】 中村 誠



## 【選任した代理人】

【識別番号】 100108855

【弁理士】

【氏名又は名称】 蔵田 昌俊

## 【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

## 【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

## 【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置及び論理演算装置

【特許請求の範囲】

【請求項 1】 入力側の複数本の信号線と、

出力側の複数本の信号線と、

前記入力側の複数本の信号線からデータを入力し、前記出力側の複数本の信号線へデータを出力する電子回路とを備え、

前記入力側の複数本の信号線から入力されるデータ及び前記出力側の複数本の信号線へ出力されるデータを、当該複数本の信号線のビット状態の組合せにより値が定まる 1 ビット・データとして扱うことを特徴とするデータ処理装置。

【請求項 2】 前記 1 ビット・データの値として 0 を与える場合の前記複数本の信号線に係る第 1 のビット状態の組合せの持つハミング重みと、前記 1 ビット・データの値として 1 を与える場合の前記複数本の信号線に係る第 2 のビット状態の組合せの持つハミング重みとを均等又は概ね均等にすることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 3】 前記複数本の信号線に係るビット状態の組み合わせとして、前記 1 ビット・データの値として 0 を与える第 1 のビット状態の組合せ又は 0 を与える第 2 のビット状態の組合せが入出力される稼働相と、無効なデータを表す前記第 1 又は第 2 のビット状態のいずれとも異なる第 3 のビット状態の組み合わせが入出力される休止相の区別を示す制御信号を入力する手段を更に備えたことを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 4】 予め定められた方法に従って前記稼働相の間に前記休止相が挿入されることを特徴とする請求項 3 に記載のデータ処理装置。

【請求項 5】 各々の前記 1 ビット・データの入出力に係る前記稼働相の間にそれぞれ前記休止相が挿入されることを特徴とする請求項 4 に記載のデータ処理装置。

【請求項 6】 前記第 3 のビット状態の組合せと前記第 1 のビット状態の組合せとの間のハミング距離と、前記第 3 のビット状態の組合せと前記第 2 のビット状態の組合せとの間のハミング距離とを均等又は概ね均等にすることを特徴と

する請求項 3 に記載のデータ処理装置。

【請求項 7】 前記入力側及び出力側の信号線の本数をそれぞれ 2 本として

、  
前記第 1 のビット状態の組合せを、当該データに係る第 1 の信号線のビット状態が 1 であり且つ第 2 の信号線のビット状態が 0 である組合せ又は第 1 の信号線のビット状態が 0 であり且つ第 2 の信号線のビット状態が 1 である組合せのいずれかとし、

前記第 2 のビット状態の組合せを、前記第 1 のビット状態の組合せを反転させた組合せとし、

前記第 3 のビット状態の組合せを、前記第 1 の信号線のビット状態が 0 であり且つ第 2 の信号線のビット状態が 0 である第 1 の組合せ及び又は前記第 1 の信号線のビット状態が 1 であり且つ第 2 の信号線のビット状態が 1 である第 2 の組合せとすることを特徴とする請求項 6 に記載のデータ処理装置。

【請求項 8】 前記データ処理装置は、同期信号を入力する手段を更に備え

、  
前記電子回路は、前記制御信号が前記稼動相を示す場合には、前記同期信号に従って、前記入力側の複数本の信号線から前記第 1 又は第 2 のビット状態の組み合わせに係る前記 1 ビット・データを入力し、前記出力側の複数本の信号線へ前記第 1 又は第 2 のビット状態の組み合わせに係る前記 1 ビット・データを出力することを特徴とする請求項 3 に記載のデータ処理装置。

【請求項 9】 前記電子回路は、前記制御信号が前記休止相を示す場合には、前記入力側の複数本の信号線から前記無効なデータを入力することなしに、前記同期信号に従って、前記出力側の複数本の信号線から前記無効なデータを出力することを特徴とする請求項 8 に記載のデータ処理装置。

【請求項 10】 前記同期信号の立ち上がり又は立ち下がりの 2 回に 1 回の割合で、前記同期信号に同期した前記 1 ビット・データが入力されることを特徴とする請求項 8 に記載のデータ処理装置。

【請求項 11】 前記電子回路は、前記 1 ビット・データを保持する回路であることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 1 2】 第 1 及び第 2 の 2 本の信号線のビット状態の組合せにより値が定まる 1 ビット・データを入力し一旦保持した後に出力する第 1 のデータ保持回路と、

第 1 及び第 2 の 2 本の信号線のビット状態の組合せにより値が定まる 1 ビット・データを入力し一旦保持した後に出力する第 2 のデータ保持回路と、

前記第 1 のデータ処理装置の出力側の第 1 の信号線を第 1 の入力データとし、前記第 2 のデータ処理装置の出力側の第 1 の信号線を第 2 の入力データとし、該第 1 の入力データ及び該第 2 の入力データをもとにした第 1 の論理演算を行って、その結果を出力する第 1 の論理演算回路と、

前記第 1 のデータ処理装置の出力側の第 2 の信号線を第 1 の入力データとし、前記第 2 のデータ処理装置の出力側の第 2 の信号線を第 2 の入力データとし、該第 1 の入力データ及び該第 2 の入力データをもとにした第 2 の論理演算を行って、その結果を出力する第 2 の論理演算回路と、

前記第 1 の論理演算回路の出力側の信号線及び前記第 2 の論理演算回路の出力側の信号線の 2 本の信号線で与えられる第 3 のビット・データを入力し一旦保持した後に出力する第 3 のデータ保持回路とを備えたことを特徴とする論理演算装置。

【請求項 1 3】 前記第 1 の論理演算回路は、前記第 1 の入力データと前記第 2 の入力データとの AND 演算を行うものであり、

前記第 2 の論理演算回路は、前記第 1 の入力データと前記第 2 の入力データとの OR 演算を行うものであることを特徴とする請求項 1 2 に記載の論理演算装置。

【請求項 1 4】 前記第 1 の論理演算回路は、前記第 1 の入力データと前記第 2 の入力データとの OR 演算を行うものであり、

前記第 2 の論理演算回路は、前記第 1 の入力データと前記第 2 の入力データとの AND 演算を行うものであることを特徴とする請求項 1 2 に記載の論理演算装置。

【請求項 1 5】 前記第 1 の論理演算回路は、前記第 1 の入力データと前記第 2 の入力データとの NAND 演算を行うものであり、

前記第2の論理演算回路は、前記第1の入力データと前記第2の入力データとのNOR演算を行うものであることを特徴とする請求項12に記載の論理演算装置。

【請求項16】 前記第1の論理演算回路は、前記第1の入力データと前記第2の入力データとのNOR演算を行うものであり、

前記第2の論理演算回路は、前記第1の入力データと前記第2の入力データとのNAND演算を行うものであることを特徴とする請求項12に記載の論理演算装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データを処理するデータ処理装置及び論理演算を行う論理演算装置に関する。

【0002】

【従来の技術】

マイクロコンピュータなどのように演算処理装置を備えたLSIにおいて、暗号演算を行う際の演算処理中の消費電力を測定し、その消費電力からLSIに納められている鍵情報を取り出すという電力差分攻撃(DPA:Differential Power Analysis)がある(例えば、非特許文献1参照)。

【0003】

DPAによる攻撃では、最初に、複数のデータをLSIに入力して、それぞれの消費電力を測定する。次に、暗号演算回路内にある鍵情報の推定を行う。この推定した鍵情報と消費電力との間に相関がある場合、その相関値を計算したとき、推定した値が正しいときに大きな相関値となり、推定が間違っているときに小さな相関値となる。DPAは、この原理を用いて、消費電力を測定することにより暗号演算回路内部の鍵情報を取り出すという攻撃方法である。

【0004】

DPAによる攻撃は、破壊行為を伴わない攻撃であるため、外見を見ただけでは攻撃され鍵情報が取り出されたかどうか判断できず、不正利用による被害が拡

大するおそれがある。このため、暗号演算回路において D P A への対策が必須となっている。

#### 【0005】

ところで、CMOS (Complementary Metal-Oxide Semiconductor) デバイスを用いて製作された演算処理装置を備えた L S I においては、同期信号を用い、1 線で 1 ビットのデータを表している。このような回路構成の L S I における消費電力は、CMOS の特性により、処理しているデータ及びその前のデータに依存して変動する。

#### 【0006】

以下、CMOS デバイスの NOT 素子の動作と消費電力について説明する。

#### 【0007】

CMOS による NOT 素子は、通常、供給電源線  $V_{cc}$ 、グランド線  $GND$ 、 $V_{cc}$  と  $GND$  との間に直列に接続された nMOS 及び pMOS、両 MOS のゲートに接続された入力信号線、nMOS と MOS との接続線に接続された出力信号線、出力信号線と  $GND$  との間に接続された容量  $C$  を備えている。

#### 【0008】

この NOT 素子の入力が高 (もしくは、1) のとき、nMOS が導通状態となるため、容量  $C$  の正の電荷は nMOS を介して  $Gnd$  に流れるため、出力の電位は low (もしくは、0) になる。ここで、high とは、演算処理装置内で論理的に 1 と認識される電位であり、low とは 0 と認識される電位である。

#### 【0009】

逆に、入力が高の場合、pMOS が導通状態となる一方で、nMOS は非導通状態となる。この pMOS が導通状態となることで、 $V_{cc}$  から正の電荷が容量  $C$  に蓄積され、出力は high となる。

#### 【0010】

入力の遷移が起こらない場合、例えば入力が high を維持する場合には、pMOS が導通状態のままであり、出力は low のままとなる。このとき、nMOS は非導通状態であるため  $GND$  に電荷は流れず、電力は消費されない。他方、



入力が low を維持する場合には、nMOS が導通状態となり、出力は high のままとなる。このとき、pMOS は非導通状態であるので、電荷が GND に流れることはなく、電力は消費されない。

#### 【0011】

このように、CMOS デバイスは、理想状態としては信号線の状態が変わらない場合には電力を消費しないため、CMOS デバイスで LSI を作ると低消費電力とすることができる。

#### 【0012】

さて、CMOS デバイスは、状態が遷移するときに、Vcc から電荷が流れ、電力を消費する。このため、入力が遷移する CMOS デバイスと、入力が遷移しない CMOS デバイスとでは、消費する電力に差が生じる。このために、信号線の状態の遷移と鍵情報との間に関係がある場合、鍵情報の演算に関して消費電力が変化する。この消費電力変動が外部から観測可能であり、このような場合、DPA により鍵情報を特定されることになる。

#### 【0013】

理想的には CMOS デバイスは信号の遷移以外に電力を消費しないが、実際には、信号の遷移による電力消費以外にも、洩れ電流という電流が流れることで、電力が消費される。この洩れ電流は、入力から pMOS 又は nMOS 1 のゲートを通りドレインに流れたり、Vcc から pMOS 及び nMOS 1 を通って GND に流れたりする電流である。この洩れ電流量は、CMOS デバイスの入力信号線と出力信号線の状態に依存する。

#### 【0014】

以上説明したように、CMOS デバイスを用いたマイクロコンピュータのデータ演算時の消費電力の変動は、信号線の状態遷移を伴わずに信号線の 0, 1 の状態に応じて消費される電力と、遷移する信号線の数とに依存して決まる。

#### 【0015】

CMOS デバイスを用いて、データを 1 ビットで表した回路構成の場合は、その前の状態により消費電力が変動することとなり、演算しているデータと消費電力との間に大きな相関を持つ。このため、鍵情報に関する演算を行っているとき

の消費電力の変動が、鍵情報と相関がある場合には、DPAによりマイクロコンピュータ内の鍵情報を推定されることとなる。

#### 【0016】

従来、DPAに対しては、演算中のデータをマスクして演算するという対策がある(例えば、特許文献1参照)。この対策は、鍵情報を用いた演算中の消費電力の変動が鍵情報と相関がなくなるように、鍵情報をマスクして演算を行うという方法である。このように鍵情報をマスクして演算することで、消費電力の変動と鍵情報との間の相関をなくすことでDPAへの対策としている。このように、消費電力の変動と鍵情報との間の相関をなくすことが、DPA対策として有効である。

#### 【0017】

しかし、この方法では、マスク演算のために余分なハードウェアあるいは計算時間が必要になる。

#### 【0018】

##### 【特許文献1】

特開 2 0 0 0 - 6 6 5 8 5

#### 【0019】

##### 【非特許文献1】

Kocher, P, Jaffe, J, and Jun, B. Differential Power Analysis. In Advances in Cryptology of CRYPTO '99 Springer-Verlag Lecture Notes in Computer Science 1666 p.388-398

#### 【0020】

##### 【発明が解決しようとする課題】

DPAによる攻撃に対する対策としては、中間データを乱数でマスクするという手段を用いずに済ませるには、演算データによらず消費電力を同じにするという対策が考えられる。中間データの値によらず常に一定の消費電力を消費するような回路構成であるならば、消費電力の変動と鍵情報との間に相関はなくなるためにDPA対策となる。このような問題を解決するために、マイクロコンピュータ内において処理しているデータや、その前のデータに依存しない回路構成が

必要となる。しかしながら、そのための技術は未だ知られていない。

#### 【0 0 2 1】

本発明は、上記事情を考慮してなされたもので、演算対象となるデータの内容によらずに消費電力を一定又は概ね一定とすることができるデータ処理装置及び論理演算装置を提供することを目的とする。

#### 【0 0 2 2】

##### 【課題を解決するための手段】

本発明に係るデータ処理装置は、入力側の複数本の信号線と、出力側の複数本の信号線と、前記入力側の複数本の信号線からデータを入力し、前記出力側の複数本の信号線へデータを出力する電子回路とを備え、前記入力側の複数本の信号線から入力されるデータ及び前記出力側の複数本の信号線へ出力されるデータを、当該複数本の信号線のビット状態の組合せにより値が定まる1ビット・データとして扱うことを特徴とする。

#### 【0 0 2 3】

好ましくは、前記1ビット・データの値として0を与える場合の前記複数本の信号線に係る第1のビット状態の組合せの持つハミング重みと、前記1ビット・データの値として1を与える場合の前記複数本の信号線に係る第2のビット状態の組合せの持つハミング重みとを均等又は概ね均等にするようにしてもよい。

#### 【0 0 2 4】

これによって、静的消費電力をデータによらず一定又は概ね一定とすることができる。

#### 【0 0 2 5】

また、好ましくは、前記複数本の信号線に係るビット状態の組み合わせとして、前記1ビット・データの値として0を与える第1のビット状態の組合せ又は0を与える第2のビット状態の組合せが入出力される稼働相と、無効なデータを表す前記第1又は第2のビット状態のいずれとも異なる第3のビット状態の組み合わせが入出力される休止相の区別を示す制御信号を入力する手段を更に備えるようにしてもよい。好ましくは、前記第3のビット状態の組合せと前記第1のビット状態の組合せとの間のハミング距離と、前記第3のビット状態の組合せと前記

第 2 のビット状態の組合せとの間のハミング距離とを均等又は概ね均等にするようにしてもよい。

#### 【0 0 2 6】

これによって、静的消費電力及び動的消費電力をデータによらず一定又は概ね一定とすることができる。

#### 【0 0 2 7】

また、本発明に係る論理演算回路は、第 1 及び第 2 の 2 本の信号線のビット状態の組合せにより値が定まる 1 ビット・データを入力し一旦保持した後に出力する第 1 のデータ保持回路と、第 1 及び第 2 の 2 本の信号線のビット状態の組合せにより値が定まる 1 ビット・データを入力し一旦保持した後に出力する第 2 のデータ保持回路と、前記第 1 のデータ処理装置の出力側の第 1 の信号線を第 1 の入力データとし、前記第 2 のデータ処理装置の出力側の第 1 の信号線を第 2 の入力データとし、該第 1 の入力データ及び該第 2 の入力データをもとにした第 1 の論理演算を行って、その結果を出力する第 1 の論理演算回路と、前記第 1 のデータ処理装置の出力側の第 2 の信号線を第 1 の入力データとし、前記第 2 のデータ処理装置の出力側の第 2 の信号線を第 2 の入力データとし、該第 1 の入力データ及び該第 2 の入力データをもとにした第 2 の論理演算を行って、その結果を出力する第 2 の論理演算回路と、前記第 1 の論理演算回路の出力側の信号線及び前記第 2 の論理演算回路の出力側の信号線の 2 本の信号線で与えられる第 3 のビット・データを入力し一旦保持した後に出力する第 3 のデータ保持回路とを備えたことを特徴とする。

#### 【0 0 2 8】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

#### 【0 0 2 9】

本発明によれば、演算対象となるデータの内容によらずに消費電力を一定又は概ね一定とすることができる。

#### 【0 0 3 0】

従って、本発明に係る装置を暗号演算回路に適用すれば、電力差分攻撃へ対策

することができる。

#### 【0 0 3 1】

##### 【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

#### 【0 0 3 2】

最初に、本実施形態の基本的な構成について説明する。

#### 【0 0 3 3】

本実施形態では、データパス部のハミング重みを一定（または、ほぼ一定）にするために、従来は1本の信号線で1ビットを表現していたものを、1ビットのデータを表すのに信号線を2本以上用いる。

#### 【0 0 3 4】

すなわち、n（nは2以上）本の信号線で与えられるデータを、nビットのデータとして扱うのではなく、当該n本の信号線のビット状態の組合せにより値が定まる1ビット・データとして扱う。

#### 【0 0 3 5】

なお、以下では、1ビットのデータを表すのに信号線を2本用いる構成を中心に説明する。

#### 【0 0 3 6】

従来のように1本の信号線で1ビットのデータを表す場合、信号線の1または0の状態がそのまま1ビットのデータの値に対応するが、1ビットのデータを表すのに2本の信号線を用いて表現する場合のデータの表現方法としては、2本の信号線を組み合わせて、1線式において“h i g h（もしくは、1）”と表した状態（当該ビットの値＝1に対応する状態）を2線式では（1，0）と符号化して表し（すなわち、第1の信号線が状態1をとり、第2の信号線が状態0をとる）、1線式において“l o w（もしくは、0）”と表した状態（当該ビットの値＝0に対応する状態）を（0，1）と符号化して表す（すなわち、第1の信号線が状態0をとり、第2の信号線が状態1をとる）、といった表現方法を導入する。もちろん、1線式において“1”と表した状態を2線式では（0，1）で、“0”と表した状態を（1，0）で表す表現方法も可能である。これらの場合、デ

ータパス部のハミング重みは1で一定となる。

#### 【0037】

このようにデータパス部のデータを符号化し、1ビットを2本の信号線で表すという2線化を行うことで、CMOSデバイスを用いて製作された演算処理装置内において、データの内容にかかわらずに、鍵情報を演算するデータパス部における状態1を持つ信号線の数と、状態0を持つ信号線の数とを等しくすることができる。

#### 【0038】

データパス部におけるハミング重み（状態1を持つ信号線の数）を一定にすることができる理由を説明する。従来のように1線で1ビットを表す1線式では、ビット値=0を表すときのハミング重みは0となり、ビット値=1を表すときのハミング重みは1となる。他方、本実施形態のように例えば2本の信号線で1ビットを表現する2線式では、ビット値=0を表すときのハミング重みとビット値=1を表すときのハミング重みはいずれも1となる。このように、2線式では、データの内容にかかわらずにハミング重みは同じ値になるため、データパス部のハミング重みは演算中に一定となるのである。

#### 【0039】

信号線の遷移に伴わずに消費される電力（スタティック消費電力）は、データパス部のハミング重みに依存することから、2線式にすることでデータによらずスタティック消費電力を一定とすることが可能となる。これによって、スタティック消費電力と鍵情報との間の相関をなくすることができる。

#### 【0040】

従って、このような構成を暗号演算回路に適用すれば、電力差分攻撃へ対策することができる。

#### 【0041】

また、本実施形態では、次のようにデータが有効であるフェイズ（稼働相）とデータが無効であるフェイズ（休止相）とを設ける2相方式を採用すると好ましい。

#### 【0042】

まず、上記のように符号化された有効なデータがデータパス部を流れるときを稼働相とする。また、状態遷移する信号線の数を一一定（または、ほぼ一定）にするため無効なデータ（非データ）がデータパス部を流れるときを休止相とする。

#### 【0 0 4 3】

例えば、2 線式において、1 ビットのデータが上記のように（1， 0）または（0， 1）で表されるのに対して、それらのいずれとの間の遷移についてもハミング距離を同じくする（0， 0）または（1， 1）を非データとする。（0， 0）は第 1 及び第 2 の信号線がいずれも状態 0 をとり、（1， 1）は第 1 及び第 2 の信号線がいずれも状態 1 をとるものである。

#### 【0 0 4 4】

このように、稼働相のときにデータを流し、休止相のときに非データを流すようにすることで、休止相を挟んで隣接するデータ間の依存関係をなくすることができる。これは、休止相により 1 ビットを表す 2 本の信号線が（0， 0）または（1， 1）という非データを表す状態に遷移するため、後続するデータは、直前のデータ（休止相を挟んで隣接するデータ）とは無関係となり、休止相にある非データとの間の相違だけで関係するからである。

#### 【0 0 4 5】

また、2 線化された信号線を（1， 0）または（0， 1）という本来のデータの状態から一旦（0， 0）または（1， 1）という本来のデータではない非データの状態に遷移させることで、データの内容によらずに 1 から 0 または 0 から 1 へ状態遷移する信号線の数を一一定にし、これによって、データの内容によらず信号線の遷移による消費電力（ダイナミック消費電力）を一一定とすることができる。この結果、ダイナミック消費電力と鍵情報との間の相関をなくすることができる。

#### 【0 0 4 6】

従って、このような構成を暗号演算回路に適用すれば、電力差分攻撃へ対策することができる。

#### 【0 0 4 7】

ここで、稼働相と休止相とを例えば交互に設けた場合を考える。例えば、図 2

にあるように、同期信号 C L K の立ち上がりのタイミングに合わせて、制御信号線を h i g h , l o w と交互に繰り返すようにし、この制御信号に従ってデータパス部を稼働相と休止相が交互に繰り返すようにする（なお、図 2 では稼働相と休止相とを同期信号 C L K の立ち下りのタイミングで切り替えたが、同期信号 C L K の立ち下りのタイミングで切り替えるようにしてもよい）。

#### 【0 0 4 8】

この場合、稼働相における信号線の状態は ( 1 , 0 ) または ( 0 , 1 ) であり、休止相における信号線の状態は ( 0 , 0 ) または ( 1 , 1 ) であるので、遷移状態としては、稼働相から休止相への遷移では、( 1 , 0 ) → ( 0 , 0 ) 、 ( 1 , 0 ) → ( 1 , 1 ) 、 ( 0 , 1 ) → ( 0 , 0 ) 、または ( 0 , 1 ) → ( 1 , 1 ) 、休止相から稼働相への遷移では、( 0 , 0 ) → ( 1 , 0 ) 、 ( 0 , 0 ) → ( 0 , 1 ) 、 ( 1 , 1 ) → ( 1 , 0 ) 、 ( 1 , 1 ) → ( 0 , 1 ) となり、いずれも、状態遷移する信号線の数は 1 つで一定となる。

#### 【0 0 4 9】

なお、上記した 2 線式 2 相方式の回路構成において、同期信号の立ち上がり（または、立ち下り）において休止相とするために、データを保持するレジスタは、休止相のデータを内部で保持しないように、入力信号を監視し、休止相であり非データを検出した場合には、レジスタの入力を内部に取り込まないようにし、他方、稼働相のデータを検出した場合には、同期信号の立ち上がり（または、立ち下り）において入力を内部に取り込むようにするという回路構成にするのが望ましい。

#### 【0 0 5 0】

また、休止相または稼働相を示す制御信号線を用意し、休止相の場合にはデータパス部に非データが流れるようにレジスタの出力部に A N D 素子または O R 素子を入れ、制御信号線に応じて、非データがレジスタの先にある組合せ回路へ入力されるようにしてもよい。

#### 【0 0 5 1】

以下では、2 線式 2 相方式の回路の具体例をいくつか示す。

#### 【0 0 5 2】



最初に、稼働相において入力データを内部に保持し、休止相においては入力データを取り込まない2線式2相方式のデータ保持回路（レジスタ）の構成例について説明する。

#### 【0053】

図1に、2線化されたデータを保持するデータ保持回路の構成例を示す。本データ保持回路は、第1のレジスタ1と、第2のレジスタ2と、監視回路3と、第1のAND回路6と、第2のAND回路7とを含む。監視回路3は、OR回路4とAND回路5とを含む。なお、図3に、第1及び第2のレジスタ1，2として使用可能な、1つのAND回路11と6つのNAND回路12～17からなるエッジトリガ型Dフリップフロップの例を示す。また、レジスタ1，2には、マスタースレーブ型Dフリップフロップを用いることも可能である。

#### 【0054】

なお、本データ保持回路は、非データ（0，0）を休止相とする場合の例である。もちろん、図1を修正すれば非データ（1，1）を休止相とする場合も実現可能である。

#### 【0055】

図1において、制御信号CTRLと同期信号CLKには、例えば図2の信号がそれぞれ供給される（本例の場合、CTRLがhighのとき稼働相となり、lowのとき休止相となる）。

#### 【0056】

図1に示されるように、2線に符号化されたデータを保持するために、従来の1線式で使われるDフリップフロップを用いて実現することができる。このように2つのDフリップフロップ1，2を並べることで、2線に符号化されたデータを保持することができる。

#### 【0057】

監視回路9は、休止相であることを監視するための回路である。すなわち、例えばデータバス部の信号線が（0，0）になる場合が休止相とした場合、監視回路9は図1のようにOR回路4とAND回路5で実現することができる。なお、（1，1）を休止相とした場合には、NAND素子とAND素子で実現すること

ができる。

#### 【0058】

第1のAND回路6及び第2のAND回路7の出力が、当該2線式の出力となる。図1の例では、稼動相において、(1, 0)または(0, 1)が出力され、休止相において(0, 0)が出力される。

#### 【0059】

図4に、本データ保持回路の動作を表すタイミングチャート例を示す。なお、図4において、(I 1, I 2)は図1の入力I 1, I 2の各状態を示し、(R 1, R 2)は図1の各レジスタ1, 2の保持状態を示し、(O 1, O 2)は図1の出力O 1, O 2の各状態を示す。稼動相で入力された入力データは、次の休止相の間も保持され(すなわち、休止相の非データは取り込まれない)、次の稼動相で出力されることがわかる。

#### 【0060】

以上のように本構成例によれば、休止相において非データを取り込まず、稼働相においてデータを保持し、稼動相においてデータを出力し、休止相において非データを出力するようなデータ保持回路を実現することができる。

#### 【0061】

ところで、データ保持回路の実現方法としては、図1の構成例のように既存の1線式で用いられているDフリップフロップを用いて実現する方法もあるが、これよりも少ない論理素子で実現することも可能である。

#### 【0062】

図5に、この場合のデータ保持回路の構成例を示す。図5に示されるように、本データ保持回路は、OR回路o r 1、AND回路a 1～a 4、NAND回路n a 1～n a 6を含む(なお、OR回路o r 1とAND回路a 1で監視回路3を形成している)。

#### 【0063】

なお、図5は、休止相が(0, 0)である場合の構成例を示しているが、もちろん、図5を修正すれば休止相が(1, 1)である場合も実現可能である。

#### 【0064】

ここで、図 6 及び図 7 を用いて、図 5 に例示した 2 線式 2 相方式のデータ保持回路の動作について詳しく説明する。なお、図 6 及び図 7 では、図 5 の AND 回路 a 3, a 4 は省略している。

#### 【0 0 6 5】

最初に図 5 の回路が休止相の状態にあるとし、入力 I 1, I 2 とともに 0 であったとする。

#### 【0 0 6 6】

次いで稼働相に遷移し、図 6 のように入力 I 2 が“1”に遷移したとすると、o r 1 の出力は“0”から“1”に遷移する。そして図 6 のように同期信号 C L K が“0”から“1”に立ち上がることで、AND 素子 a 1 の出力が“0”から“1”に遷移する。これにより、NAND 素子 n a 2 の出力が“1”から“0”に遷移する。AND 素子 a 2 の出力は、“0”となり NAND 素子 n a 3 の出力は“1”に遷移する。以上の動作で、NAND 素子 n a 5 の出力は“1”となり、NAND 素子 n a 6 の出力は“0”となる。NAND 素子 n a 5, n 6 の出力を AND 素子 a 4, a 3 の入力に入れ、制御信号 C T R L との AND 演算を行うことで、稼働相におけるデータ (0, 1) が出力される。

#### 【0 0 6 7】

さらに稼働相から休止相へ遷移し、図 7 のように入力 I 2 が“1”から“0”に遷移する。この結果、OR 素子 o r 1 の出力は“0”になり、AND 素子 a 1, a 2 の出力も“0”となる。AND 素子 a 1 の出力が“0”になることで、NAND 素子 n a 2 の出力は“1”となり、NAND 素子 n a 3 の出力も“1”となる。このとき、NAND 素子 n a 5, NAND 素子 n a 6 の出力は変わらない。NAND 素子 n a 5, n 6 の出力は AND 素子 a 4, a 3 の入力に入れられるが、制御信号 C T R L との AND 演算が行われるので、稼働相におけるデータ (0, 0) が出力される。

#### 【0 0 6 8】

以上に示したように、図 5 のような回路構成とすることで、休止相において入力を取り込まず以前の稼働相のデータを保持し続け、稼働相において入力データを内部に取り込むような 2 線式用の 1 ビットのデータ保持回路を構成することが

できる。

#### 【0 0 6 9】

このようなレジスタを用い、稼働相と休止相を交互に流すことで、データパス部のハミング重みが一定となるとともに、信号線の遷移数が一定になることについて説明する。

#### 【0 0 7 0】

スタティック消費電力においては、データのハミング重みが問題となる。2線式のデータパス部において、1ビットのデータは(1, 0)または(0, 1)と表現される。例えば、1線式において、8ビットのデータ0 x 1 8 (0 0 0 1 1 0 0 0)についてはハミング重みは“2”、0 x f f (1 1 1 1 1 1 1 1)についてはハミング重みは“8”となる。一方、2線式においては、8ビットのデータ0 x 1 8は(0, 1) (0, 1) (0, 1) (1, 0) (1, 0) (0, 1) (0, 1) (0, 1)と表されるために、そのハミング重みは“8”であり、0 x f fは(1, 0) (1, 0) (1, 0) (1, 0) (1, 0) (1, 0) (1, 0) (1, 0)と表されるために、そのハミング重みは同じく“8”となる。

#### 【0 0 7 1】

このように、1線式ではデータの内容によってハミング重みが異なるが、2線式では1ビットのデータを2線で(1, 0)または(0, 1)で表すために、データの内容にかかわらずにハミング重みは一定となる。

#### 【0 0 7 2】

次に、図8に、1ビットの論理AND演算を行う2線式データパス部の構成例を示す。

#### 【0 0 7 3】

図8に示されるように、本演算回路は、本実施形態のデータ保持回路r 1 ~ r 3と、AND回路a 1と、OR回路o r 1とを含む。

#### 【0 0 7 4】

以下、図8に例示した1ビットの論理AND演算を行う2線式データパス部を用いて、ダイナミック消費電力について説明する。

#### 【0 0 7 5】

ここでは、1ビットのデータの値＝1を（1，0）で表し、1ビットのデータの値＝0を（0，1）で表すものとする。また、休止相を（0，0）とする。また、制御信号CTRLと同期信号CLKには図2の信号がそれぞれ供給されるものとする（CTRLがhighのとき稼働相となり、lowのとき休止相となるものとする）。

#### 【0076】

まず、図9の状態において、レジスタr1に（0，1）、レジスタr2に（1，0）、レジスタr3に（1，0）がそれぞれ保持されており、休止相（制御信号は“0”）であったとする。この状態では、全ての信号線の状態が“0”になっている。

#### 【0077】

次に、休止相から稼働相へ遷移し（制御信号は“0”から“1”に遷移し）、図10の状態になったものとする。この状態では、レジスタr1へ（1，0）、レジスタr2へ（1，0）がそれぞれ入力されたものとする。また、レジスタr1から（0，1）、レジスタr2から（1，0）がそれぞれ出力され、それらが2線式のデータに対する論理AND演算を行う組合せ回路a1，or1に入力され、その演算結果（0，1）が出力され、これがレジスタr3に届き、保持される。また、レジスタr3からは、（1，0）が出力される。

#### 【0078】

ここで、図9の状態から図10の状態への遷移をみると、組合せ回路の6つ信号線のうちの3つの信号線において状態が“0”から“1”に遷移していることがわかる。

#### 【0079】

次に、稼働相から休止相へ遷移し（制御信号は“1”から“0”に遷移し）、図9の状態に戻ったものとする。この状態では、全ての信号線の状態が“0”になっている。

#### 【0080】

ここで、図10の状態から図9の状態への遷移をみると、やはり3つの信号線において状態が遷移していることがわかる。

**【0081】**

次に、休止相から稼働相へ遷移し（制御信号は“0”から“1”に遷移し）、図11の状態になったものとする。この状態では、レジスタ r1へ（0，1）、レジスタ r2へ（0，1）がそれぞれ入力されたものとする。また、レジスタ r1から（1，0）、レジスタ r2から（1，0）がそれぞれ出力され、それらが2線式のデータに対する論理AND演算を行う組合せ回路 a1，o r1に入力され、その演算結果（1，0）が出力され、これがレジスタ r3に届き、保持される。また、レジスタ r3からは、（0，1）が出力される。

**【0082】**

ここで、図9の状態から図11の状態への遷移をみると、やはり3つの信号線において状態が遷移していることがわかる。

**【0083】**

このように、データの内容にかかわらずに、遷移する信号線の数是一定になる。

**【0084】**

このように、稼働相と休止相によりデータと非データを交互にデータパスに流すことで、データパス部における組合せ回路の信号線のうち状態遷移するものの個数は一定となり、ダイナミック消費電力は一定となる。

**【0085】**

ところで、図8では1ビットの論理AND演算を行う2線式データパス部の構成例を示したが、もちろん、この構成例を適宜修正することによって、他の論理演算を行う2線式データパス部も実現可能である。

**【0086】**

図12に、1ビットの論理OR演算を行う2線式データパス部の構成例を示す。図12に示されるように、本演算回路は、本実施形態のデータ保持回路 r1～r3と、OR回路 o r2とAND回路 a2とを含む。

**【0087】**

また、図13に、1ビットの論理NAND演算を行う2線式データパス部の構成例を示す。図13に示されるように、本演算回路は、本実施形態のデータ保持

回路  $r_1 \sim r_3$  と、NAND回路  $na_1$  と、NOR回路  $nor_1$  とを含む。

【0088】

また、図14に、1ビットの論理NOR演算を行う2線式データパス部の構成例を示す。図14に示されるように、本演算回路は、本実施形態のデータ保持回路  $r_1 \sim r_3$  と、NOR回路  $nor_2$  とNAND回路  $na_2$  とを含む。

【0089】

また、図15に、1ビットの論理NOT演算を行う2線式データパス部の構成例を示す。図15に示されるように、本演算回路は、本実施形態のデータ保持回路  $r_1$ 、 $r_2$  とを含み、データ保持回路  $r_1$  の第1の出力  $O_1$  をデータ保持回路  $r_2$  の第2の入力  $I_1$  へ結合し、データ保持回路  $r_1$  の第2の出力  $O_2$  をデータ保持回路  $r_2$  の第1の入力  $I_2$  へ結合するものである（図中、 $h_1$  の配線部分参照）。なお、この場合、1ビットの論理NOT演算を行う2線式データパス部は、図16に示すように、2つのNOT回路  $not_1$ 、 $not_2$  を用いても実現可能である。

【0090】

なお、これまでの説明では、非データ（0，0）を休止相とする場合を中心に説明したが、非データ（1，1）を休止相とする場合も実現可能であり、また、休止相に非データ（0，0）と（1，1）を併用する（例えば、交互あるいはランダムに使用する）構成も可能である。

【0091】

また、これまでの説明では、稼動相と休止相とを交互に設ける場合を中心に説明したが、所定回数の稼動相が続いた後に休止相を設ける、休止相をランダムに設けるなど、それ以外の構成も可能である。

【0092】

また、これまでの説明では、1ビットのデータを表すのに信号線を2本用いる構成を中心に説明したが、1ビットのデータを表すのに信号線を3本以上用いる構成も可能である。

【0093】

1ビットのデータを表すのに4本の信号線を用いる場合には、例えば、状態1

を (1, 1, 0, 0)、状態 0 を (0, 0, 1, 1) で表し、5 本の信号線を用いる場合には、例えば、状態 1 を (1, 0, 1, 0, 1)、状態 0 を (0, 1, 0, 1, 0) で表すなどすればよい。

#### 【0 0 9 4】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

#### 【0 0 9 5】

##### 【発明の効果】

本発明によれば、演算対象となるデータの内容によらずに消費電力を一定又は概ね一定とすることができる。

##### 【図面の簡単な説明】

【図 1】 本発明の一実施形態に係るデータ保持回路の構成例を示す図

【図 2】 同実施形態における同期信号と制御信号のタイミングの一例を示す図

【図 3】 同期信号を用いた 1 線式の 1 ビットの D フリップフロップの構成例を示す図

【図 4】 同実施形態に係るデータ保持回路の動作例を示す図

【図 5】 本発明の一実施形態に係るデータ保持回路の他の構成例を示す図

【図 6】 図 5 のデータ保持回路の動作について説明するための図

【図 7】 図 5 のデータ保持回路の動作について説明するための図

【図 8】 同実施形態に係る論理 AND 演算を行うデータパス部の構成例を示す図

【図 9】 図 8 のデータパス部の動作について説明するための図

【図 1 0】 図 8 のデータパス部の動作について説明するための図

【図 1 1】 図 8 のデータパス部の動作について説明するための図



【図 1 2】 同実施形態に係る論理 O R 演算を行うデータパス部の構成例を示す図

【図 1 3】 同実施形態に係る論理 N A N D 演算を行うデータパス部の構成例を示す図

【図 1 4】 同実施形態に係る論理 N O R 演算を行うデータパス部の構成例を示す図

【図 1 5】 同実施形態に係る論理 N O T 演算を行うデータパス部の構成例を示す図

【図 1 6】 同実施形態に係る論理 N O T 演算を行うデータパス部の他の構成例を示す図

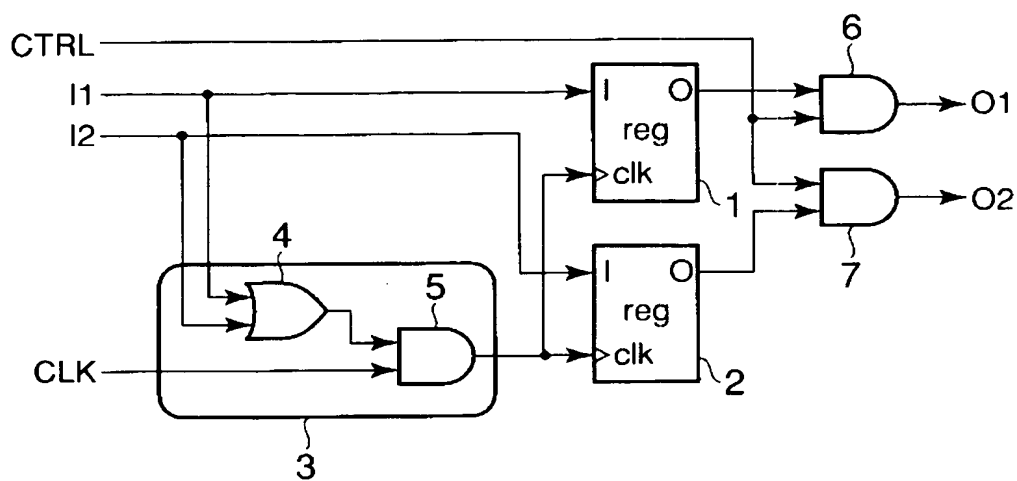
【符号の説明】

1, 2…レジスタ、3…監視回路、5, 6, 7, 11, a1～a4…AND回路、4, o r 1, o r 2…OR回路、12～17, n a 1～n a 6…NAND回路、n o r 1, n o r 2…NOR回路、n o t 1, n o t 2…NOT回路、r 1～r 3…データ保持回路

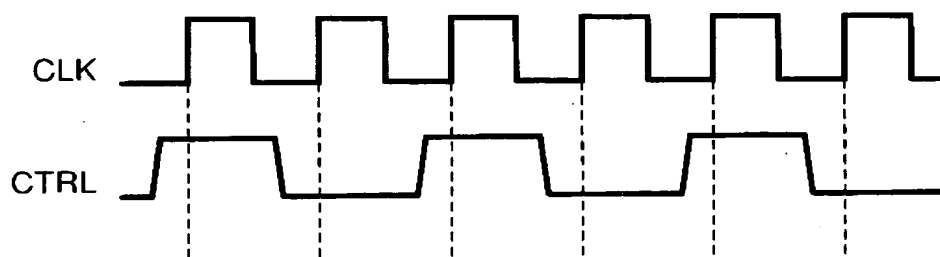
【書類名】

図面

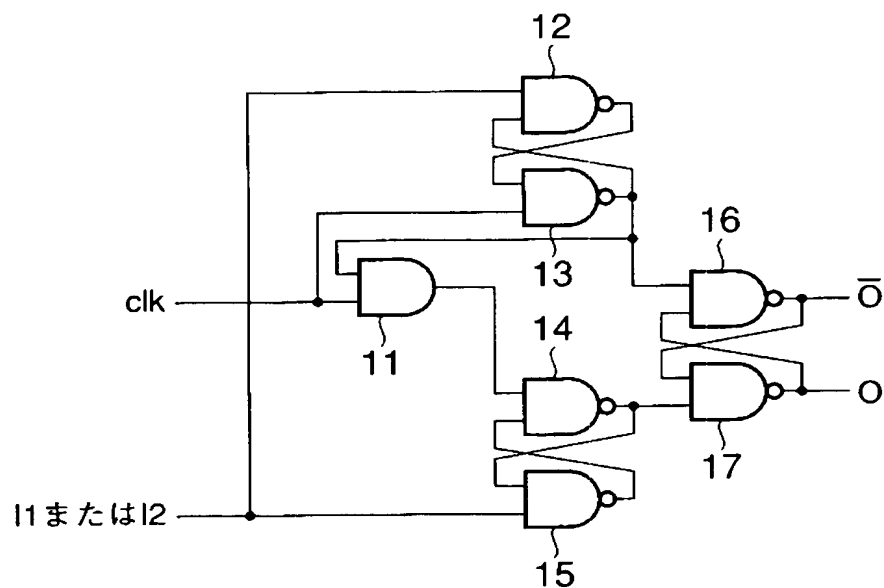
【図 1】



【図 2】



【図 3】



【図 4】

(11,12)

|     |       |       |       |       |     |
|-----|-------|-------|-------|-------|-----|
| ... | (0,1) | (0,0) | (1,0) | (0,0) | ... |
|-----|-------|-------|-------|-------|-----|

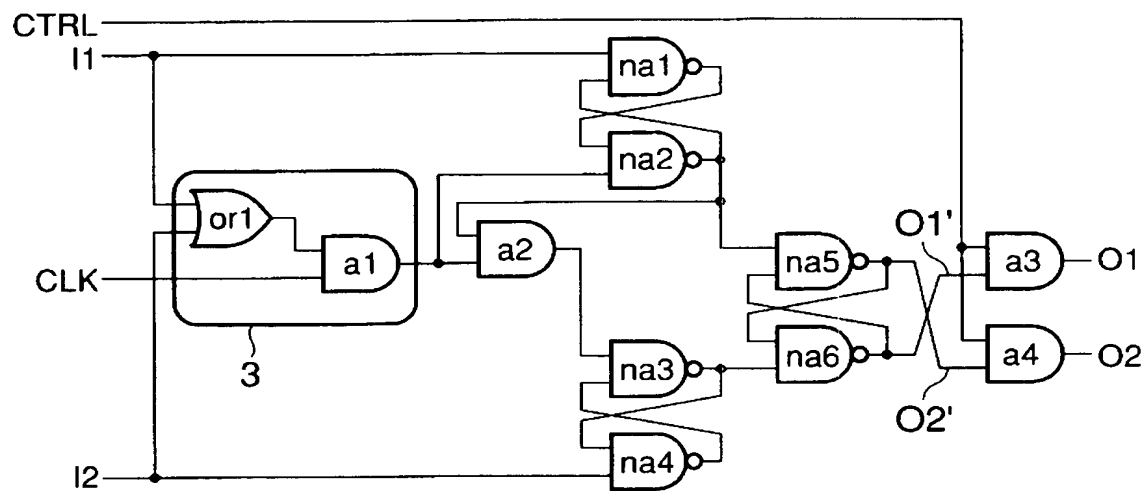
(R1,R2)

|     |       |       |     |
|-----|-------|-------|-----|
| ... | (0,1) | (1,0) | ... |
|-----|-------|-------|-----|

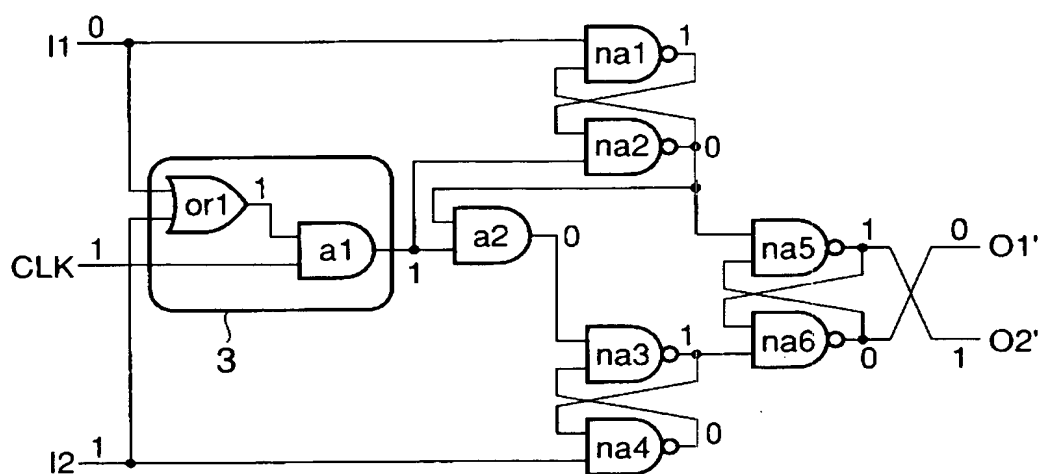
(01,02)

|     |       |       |       |       |     |
|-----|-------|-------|-------|-------|-----|
| ... | (0,0) | (0,1) | (0,0) | (1,0) | ... |
|-----|-------|-------|-------|-------|-----|

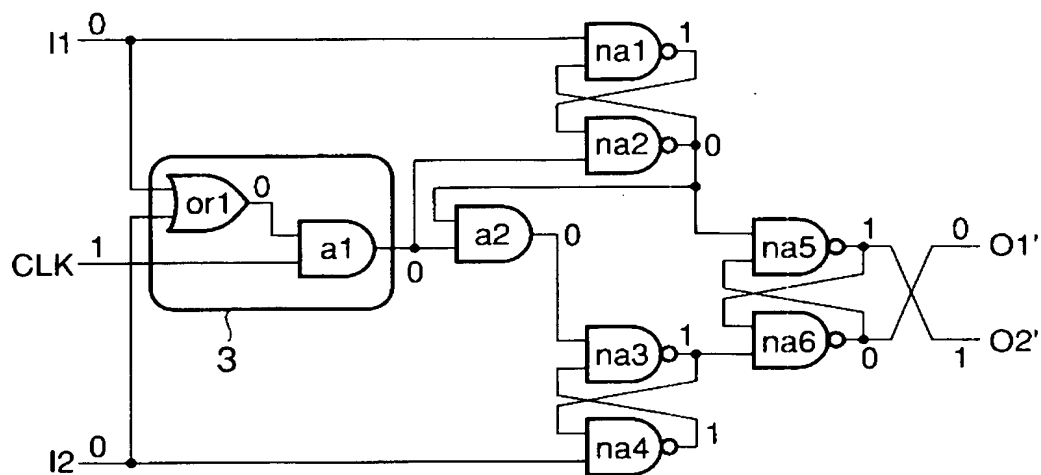
【図 5】



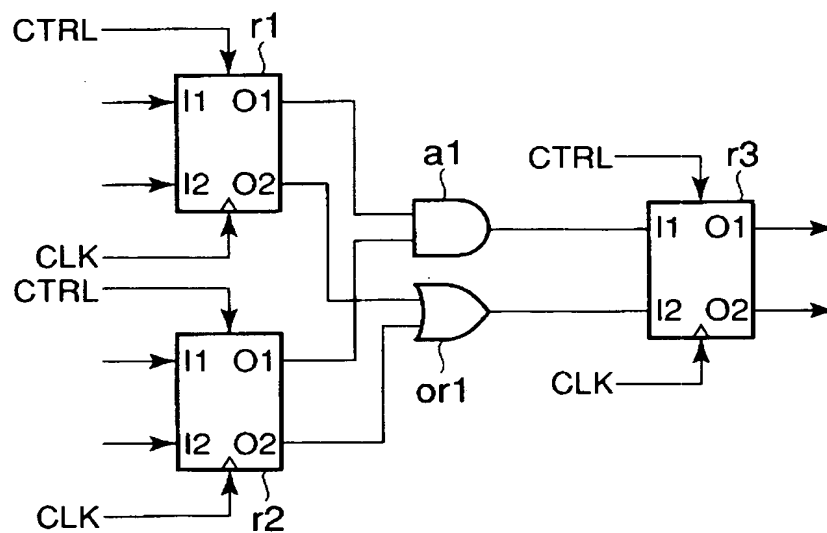
【図 6】



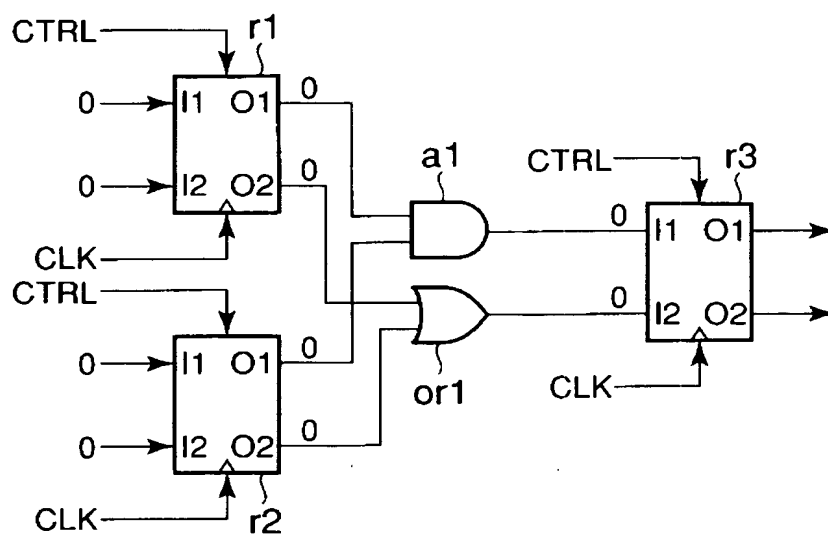
【図 7】



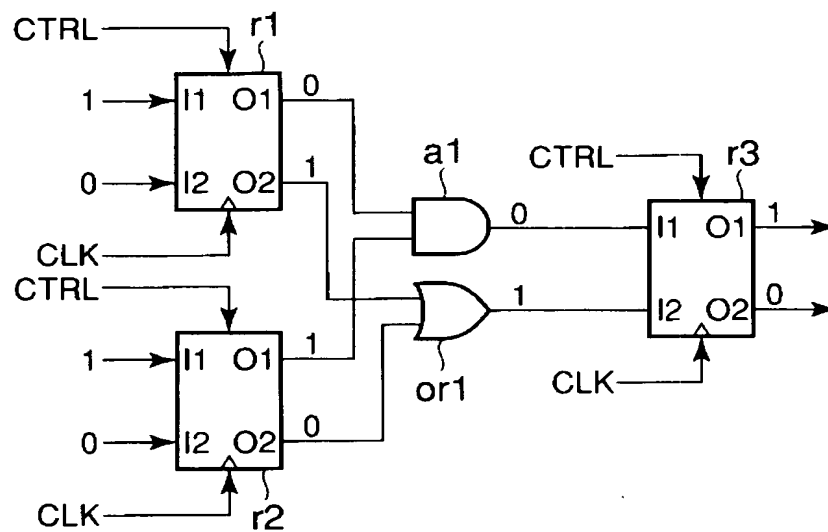
【図 8】



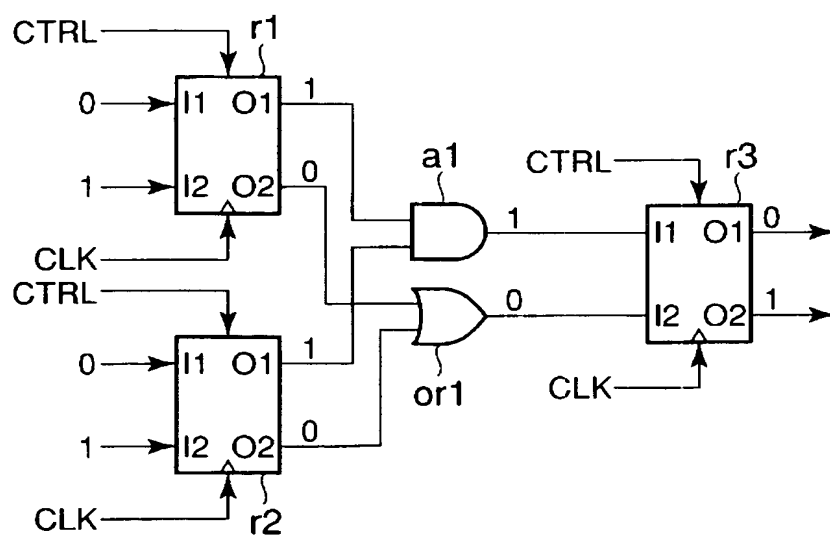
【図 9】



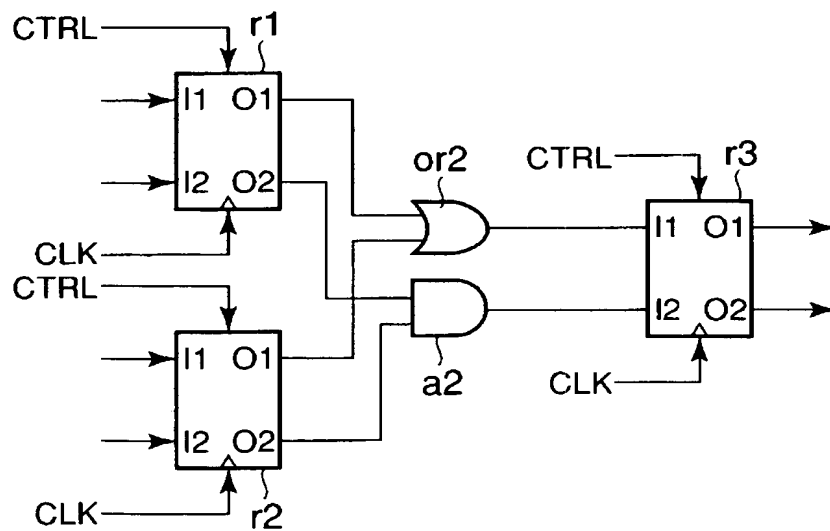
【図 10】



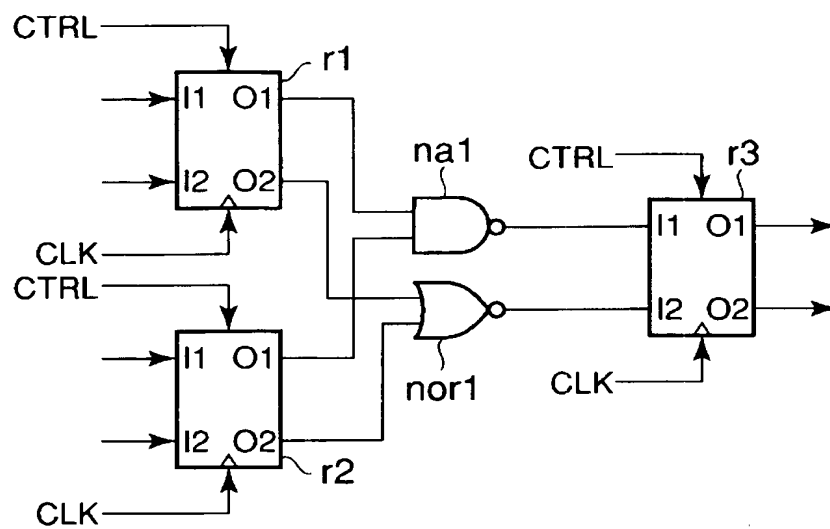
【図 1 1】



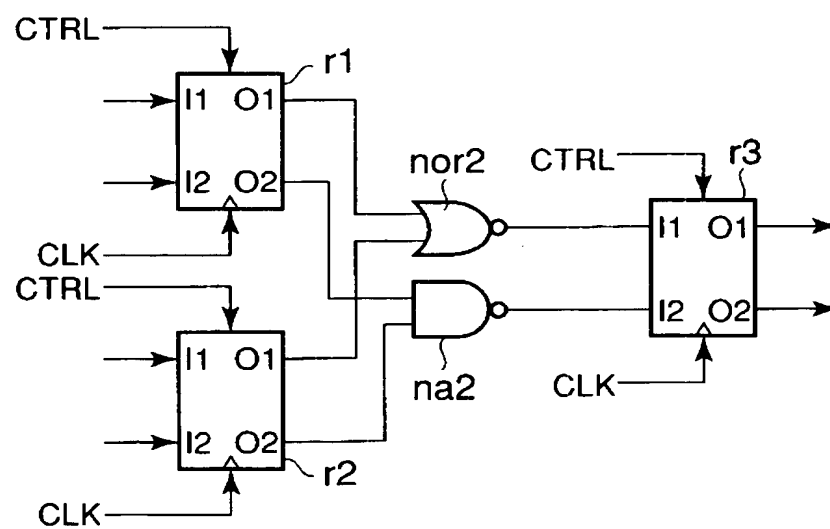
【図 1 2】



【図 13】

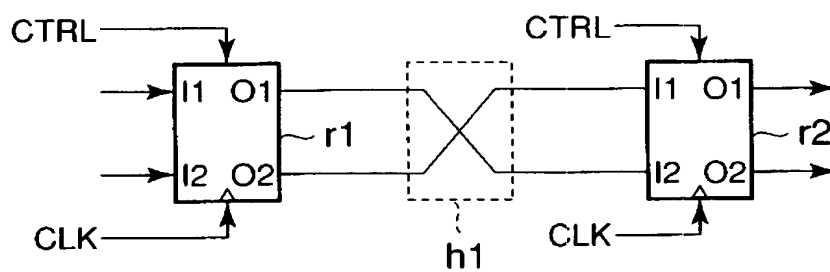


【図 14】

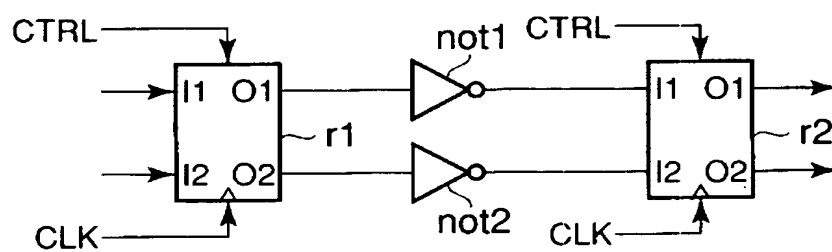




【図 15】



【図 16】



【書類名】 要約書

【要約】

【課題】 演算対象となるデータの内容によらずに消費電力を一定とすることができるデータ処理装置を提供すること。

【解決手段】 入力側の 2 本の信号線 I 1, I 2 あるいは出力側の 2 本の信号線 O 1, O 2 の状態が (1, 0) である場合を値 1 を持つ 1 ビット・データとし、(0, 1) である場合を値 0 を持つ 1 ビット・データとし、レジスタ 1, 2 は、C T L R 信号が h i g h の状態で、(1, 0) 又は (0, 1) で表される 1 ビット・データを C L K 信号に従って入力し一旦保持するとともに、保持していた (1, 0) 又は (0, 1) で表される 1 ビット・データを出力する。他方、C T L R 信号が l o w の状態では、(0, 0) で表される無効なデータが与えられるが、レジスタ 1, 2 は、該無効なデータは取り込まない。また、このとき、A N D 回路 6, 7 により、無効なデータ (0, 0) が出力される。

【選択図】 図 1

特願 2 0 0 3 - 1 4 6 4 9 1

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 3 0 7 8 ]

1. 変更年月日

2 0 0 1 年 7 月 2 日

[変更理由]

住所変更

住 所

東京都港区芝浦一丁目 1 番 1 号

氏 名

株式会社東芝